Policy: 01-12-01

Credit Card Processing (PCI DSS)

OFFICE OF RECORD: Business Office
ISSUED BY: Vice President for Business Affairs
APPROVED BY: *Douglas D. Knowlton, Pres*
EFFECTIVE DATE: 11/01/2010

Purpose

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, Dakota State University has established a formal policy for credit card processing. This policy will be evaluated on an annual basis.

Scope

This policy applies to all systems that are subject to PCI DSS requirements.

Policy

- Dakota State University staff who receive credit card information on paper will process the transaction immediately. As soon as the transaction has been processed, the credit card information will be destroyed by shredding through a cross-cut shredder.
- Credit card information shall not be sent via e-mail or other unsecured communication methods (chat, instant messaging, etc.) nor stored on any form of media such as a computer, flash drive, external hard-drive, etc.
- If it is necessary for staff to accept credit card information over the phone, the information is to be written on a piece of paper and hand-delivered to the appropriate office for processing. The paper containing the credit card information will be held in secure storage until the transaction is verified. It will then continue to be held in secure storage until it is shredded.
- Credit card information may be faxed to an office. However, the fax machine must be in a secure area. Faxed information must be immediately hand delivered to the appropriate office for processing. Any electronic memory on fax/scanning machines used to disseminate credit card information must be fully erased or physically destroyed when the equipment is retired.

- All forms will be designed so that any credit card information can be easily cut off after processing and shredded.
- Any forms containing cardholder information must be held in secure storage.
- Terminals and underlying applications must be configured to mask the PAN when displayed.
- The security code will not be requested for any transaction unless through an authorized third party service provider.
- All terminals and underlying systems must be configured to truncate account numbers on printed copies of receipts.
- Recurring payments will be handled by the credit card service provider and will not require access to the PAN by DSU staff.